

| [NODIS Library](#) | [Legal Policies\(2000s\)](#) | [Search](#) |



# NASA Policy Directive

**NPD 2540.1G**

Effective Date: June 08, 2010

Expiration Date: June 08, 2015

**COMPLIANCE IS MANDATORY**[Printable Format \(PDF\)](#)

Request Notification of Change

(NASA Only)

## **Subject: Personal Use of Government Office Equipment Including Information Technology**

**Responsible Office: Office of the Chief Information Officer**

### **1. POLICY**

a. It is NASA's policy to permit limited personal use of Government office equipment, including information technology (IT). The intent is to provide a professional and supportive work environment while meeting taxpayer expectations that tax dollars be spent wisely. By authorizing limited personal use of Government office equipment, NASA assumes that employees and contractors are responsible individuals, capable of balancing this privilege with the expectations of American taxpayers.

b. The limited personal use of Government office equipment by NASA employees and contractors shall not interfere with official business, violate existing laws, and should involve only minimal additional expense to the Government. The privilege to use Government office equipment for non-Government purposes may be revoked or limited at any time by appropriate Federal or Agency officials. Individual NASA Centers and contractors may invoke more stringent policies.

This policy in no way limits Agency employees' use of Government office equipment including IT, for official activities.

c. Specific Provisions - Employees are authorized limited personal use of Government office equipment to the extent that such personal use does not interfere with official duties or result in a loss of employee productivity. Employees must be authorized to use the office equipment for official business before it is available for personal use. NASA is not required to supply employees with equipment if it is not required for the employee to perform official business. Moreover, personal use should incur only minimal additional expense to the Government in areas such as:

(1) Communications infrastructure costs such as telephone or airtime charges, Internet

connectivity, telecommunications traffic, etc. However, an authorized personal long distance toll call may be made at Government expense to locations within the local commuting area to speak to a spouse or dependent (or those responsible for their care), to reach a number only available during working hours (such as a local Government agency, physician, or dentist), or to arrange for emergency repairs to the employee's residence or property.

(2) Consumables such as paper, ink, toner, etc.

(3) Wear and tear on equipment such as copiers, printers, etc. (4) Impacts to network bandwidth such as moderate e-mail message sizes (e-mails with small attachments), text messaging, and personal use of social media (e.g., Twitter, Facebook, YouTube).

d. Inappropriate Personal Use - Employees are expected to conduct themselves professionally in the workplace and to refrain from using Government office equipment for activities that are inappropriate. Misuse or inappropriate use of Government office equipment includes:

(1) Any personal use that violate applicable law, Agency policies, or procedural requirements.

(2) Any personal use that could cause unnecessary congestion, delay, or disruption of service to any Government system or component.

(3) Using a Government system as a staging ground or platform to gain unauthorized access to other systems.

(4) The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of subject matter.

(5) Activities inconsistent with the Federal Standards of Ethical Conduct or Equal Opportunity laws and regulations. This includes material that is inappropriate or offensive based on race, color, national origin, sex, religion, age, disability, genetic information, sexual orientation, gender identity, or status as a parent.

(6) Creating, searching/downloading, viewing, storing, copying, or transmission of materials describing or depicting sexually explicit conduct, as defined by 18 USC § 2256, Sexual Exploitation and Other Abuse of Children, or other sexually explicit or sexually oriented materials.

(7) Use for commercial purposes, "for profit" activities, or in support of outside employment or business activity such as a personal business, or assisting friends, relatives, or others in such activities (e.g., consulting for pay, sales or administration of business transactions, and sale of goods or services).

(8) Engaging in a personal or private capacity in any outside fund- raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited political activity (e.g., expressing opinions about candidates, distributing campaign literature).

(9) Publicly communicating Agency information, including Agency policy, project, or program information and other critical data, that has not been authorized for release. This includes uses that could create the perception that the communication was made on behalf of the Agency or the Office of the Administrator if the communication has not been authorized by the Office of Communications. Authorized public communications of

Agency information are subject to 14 C.F.R. section 1213 and applicable Agency policies.

(10) Any use that could generate more than minimal additional expense to the Government.

(11) The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information, including computer software and data, that includes privacy information, copyrighted, trademarked, or material with other intellectual property rights (such as literature, music, and videos beyond fair use), proprietary data, or export controlled software or data.

(12) Unauthorized peer-to-peer (P2P) file sharing activities.

(13) Overriding or defeating a security feature of a Government system (e.g., installing unapproved software).

e. Privacy Expectations - NASA employees and contractors do not have a right to expect privacy while using Government office equipment at any time, including accessing the Internet and using e-mail. Employees and contractors are advised that the Government maintains call detail and network access records to monitor telephone activity and Internet access and employs monitoring tools to track system performance and improper use. To the extent that employees and contractors wish that their private activities remain private, avoid using Government office equipment, including IT. By using Government office equipment, employees and contractors consent to disclosing the contents of any files or information maintained or passed through the equipment. Any use of Government communication resources is made with the understanding that such use is generally not secure, is not private, and is not anonymous.

f. Sanctions for Misuse - Unauthorized or improper use of Government office equipment could result in loss of use or limitations on use of equipment, disciplinary or adverse actions, criminal penalties, and/or employees/contractors being held financially liable for the cost of improper use.

g. Removing Equipment from the Workplace

(1) Domestic Travel - When IT and/or computer equipment is taken out of the workplace (i.e., telework, offsite business meetings, conferences), it is the responsibility of the employee to ensure that the equipment remains in their custody, is handled and maintained properly, and is returned in good condition. In the event that the equipment is lost, stolen, or damaged, the employee shall notify the Center Chief Information Officer (CIO) as soon as possible after the occurrence of an incident.

(2) International Travel - The employee shall use only equipment officially approved for use outside of the U.S. for international business meetings, conferences, symposia, etc. The employee must ensure that the hardware remains in their possession while outside the U.S. Any loss, damage, or tampering shall be reported immediately/at the earliest opportunity to the Center CIO. Under no circumstances should Agency laptops or personal computers be used for official business on International trips unless written authorization is first obtained from the Center CIO.

## **2. APPLICABILITY**

This NPD applies to employee and contractor personal use of Government office equipment and IT, whether owned or otherwise provided by NASA Headquarters and NASA Centers, including Component Facilities.

### **3. AUTHORITY**

- a. 5 U.S.C. § 301, Departmental Regulations, as amended.
- b. 42 U.S.C. § 2473(c)(1), Section 203(c)(1) of the National Aeronautics and Space Act of 1958, as amended.
- c. 44 U.S.C. § 3541, Federal Information Security Management Act of 2002.

### **4. REFERENCES**

- a. 18 U.S.C. § 2256, Sexual Exploitation and Other Abuse of Children.
- b. 40 U.S.C. § 11101, Information Technology Management.
- c. Executive Order No. 13011 of July 16, 1996, as amended by Executive Order No. 13284 of January 23, 2003, and Executive Order No. 13286 of February 28, 2003, Federal Information Technology.
- d. 5 C.F.R. Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch.
- e. 14 C.F.R. Part 1213, Release of Information to News and Information Media.
- f. NASA Policy Directive (NPD) 1900.9, Ethics Program Management.
- g. NASA Procedural Requirements (NPR) 1900.3, Ethics Program Management.
- h. NPR 2810.1, Security of Information Technology.
- i. Office of Management and Budget (OMB) Memorandum 04-26, Personal Use Policies and File Sharing Technology.

### **5. RESPONSIBILITY**

- a. The Office of the Chief Information Officer is responsible for development, implementation, and management of this NPD.
- b. Each Center Director and, for Headquarters, the Executive Director for Headquarters Operations, is responsible for developing procedures for ensuring that employees are aware of proper personal use of Government office equipment, including information technology, and developing cost- effective controls for monitoring or preventing abnormal or inappropriate use. Controls to be considered include blocking of inappropriate Web sites and phone numbers, flagging abnormal long distance or phone

charges, and monitoring network traffic for suspicious traffic or inappropriate use.

c. Supervisors are responsible for reasonably monitoring appropriate use of Government office equipment, including IT, and pursuing sanctions for misuse, including potential disciplinary action.

(1) Visitors and interns must be explicitly authorized to use Government office equipment and IT. Those providing this explicit permission will ensure visitors and interns are knowledgeable of Federal and Agency policy before use of the equipment or IT.

d. Employees and contractors are responsible for being knowledgeable of Federal and NASA requirements and complying with personal use privileges of Government office equipment, including IT, as outlined herein. Employees and contractors shall ensure that their personal use of Government office equipment does not give rise to an appearance that they are acting in an official capacity or that NASA endorses or sanctions their personal activities.

(1) Specific attention and care needs to be directed to participation in social media online when using Federal Government resources to access Internet-based capabilities. NASA employees and contractors bear the responsibility of using social media tools and should only engage in social networking in a responsible, safe, and judicious manner, whether in an official capacity or through personal use, to protect mission objectives, program integrity, data, and NASA's reputation. NASA managers and supervisors have the discretion to restrict personal use of social media technologies by employees during duty hours.

(2) NASA employees will distinguish between official and personal communications to ensure that all official communications are identified and conducted in conformance with applicable law, regulation, and policy, including coordination with the responsible Public Affairs Official. NASA employees will clearly identify personal communications and personal opinion (versus Agency) when using these technologies to discuss NASA and its activities.

## **6. DELEGATION OF AUTHORITY**

None.

## **7. MEASUREMENTS**

None.

## **8. CANCELLATION**

NPD 2540.1F, dated May 5, 2005.

## **/s/Charles F. Bolden Jr., Administrator**

---

### **ATTACHMENT A: (TEXT)**

#### **A. Definitions**

A.1 Privilege means, in the context of this policy, that NASA is extending the opportunity to its employees and contractors to use Government property for personal use in an effort to create a more supportive work environment. As a privilege, employees and contractors have no inherent right to personal use or ownership of Government office equipment. Nor does the privilege extend to modifying such equipment, including loading personal software or making configuration changes. This privilege may be revoked at any time, for any reason.

A.2 Government office equipment, including Information Technology (IT), includes but is not limited to: computers and related peripheral equipment and software, library resources, research or reference services (e.g., online journals), telephones and wireless communications devices (e.g., cell phones, smart-phones, pagers), personal electronic devices (e.g., calculators, music players, global positioning system devices, book readers), facsimile machines, photocopiers, office supplies, network access (e.g., Internet, wireless, cellular), e-mail, and licenses (e.g., software licenses).

A.3 IT, per United States Code (40 USC § 11101(6)).

(a) means any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by NASA directly or is used by a contractor under a contract with NASA that requires the use

(i) of that equipment; or

(ii) of that equipment to a significant extent in the performance of a service of the furnishing of a product;

(b) means any computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources;

(c) does not include any equipment acquired by a Federal contractor incidental to a Federal contract. Examples include, but are not limited to, computers and associated peripherals, software, and removable media.

A.4 Minimal additional expense means that an employee's personal use of Government office equipment is limited to those situations where the Government is already providing equipment or services and the employee's use of such equipment or services will not result in any discernable additional expense to the Government, resulting only in normal



wear and tear, or the use of small amounts of electricity, toner, ink, or paper. Examples of minimal additional expense include making occasional brief personal local phone calls, infrequently sending personal e-mail messages, making a copy of a personal bill, receiving a fax from a car repair shop, or limited use of the Internet for personal and appropriate reasons.

A.5 Personal use means uses other than for official Government business.

A.6 Peer-to-Peer file sharing, as defined in Office of Management and Budget Memo 04-026, refers to any software or system allowing individual users of the Internet to connect to each other and trade files. These systems are usually highly decentralized and are designed to facilitate connections between persons who are looking for certain types of files.

A.7 Social media technologies include, but are not limited to, wikis, blogs, mash-ups, Web feeds (e.g., Really Simple Syndication and Rich Site Summary (RSS) feeds), social networking sites (e.g., Facebook), microblogging (e.g., Twitter), and Web-based forums.

## ATTACHMENT B: REFERENCES

B.1. Executive Order 13011 of July 16, 1996, as amended by Executive Order 13284 of January 23, 2003, and Executive Order 13286 of February 28, 2003, Federal Information Technology.

B.2. Executive Order 12674 of April 12, 1989, as amended by Executive Order 12731 of October 17, 1990, Principles of Ethical Conduct for Government Officers and Employees.

B.3. 5 CFR § 2635, Standards of Ethical Conduct for Employees of the Executive Branch.

B.4. 14 CFR 1213, Release of Information to News and Information Media.

B.5. NASA Procedural Requirements (NPR) 1900.3, Ethics Program Management.

B.6. NASA Policy Directive (NPD) 1900.9, Ethics Program Management.

B.7. NPR 2810.1, Security of Information Technology.

B.8. Office of Management and Budget (OMB) Memorandum 04-26, Personal Use Policies and File Sharing Technology.

## (URL for Graphic)

## **DISTRIBUTION:** **NODIS**

---

### **This Document Is Uncontrolled When Printed.**

Check the NASA Online Directives Information System (NODIS) Library to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>

---

